Provable Ergodicity in Arithmetic Dynamics via Erdős Covering Systems

Lukas Cain

December 2, 2025

Abstract

Standard arithmetic pseudo-random number generators (PRNGs) and chaotic maps often suffer from "Dark Corners"—unreachable sub-regions of the state space or isolated attractor basins. We propose a solution rooted in Number Theory: the *Dynamic Covering Map*. By utilizing an Erdős Covering System $\mathcal{C} = \{a_i \pmod{m_i}\}_{i=1}^{k}$ where $\bigcup(a_i \pmod{m_i}) = \mathbb{Z}$, we construct a piecewise affine transformation that guarantees a valid divergent transition for every possible integer state. We prove that such systems are structurally "Backdoor-Free," ensuring ergodic traversal of the state space by algebraic necessity rather than statistical probability.

1 Introduction

A critical vulnerability in hardware security modules is the potential for hidden internal states or unreachable entropy regions. In linear systems (LFSRs), the state space is well-understood but cryptographically weak. In non-linear systems (Collatz-like maps), the state space is strong but structurally opaque; it is often unproven whether the trajectory visits the entire available space or gets trapped in localized loops.

We introduce a class of entropy sources governed by **Discrete Arithmetic Dynamics**, specifically utilizing *Covering Systems* to force global mixing.

2 Theoretical Framework

2.1 Erdős Covering Systems

A system of congruences $\{a_1 \pmod{m_1}, \dots, a_k \pmod{m_k}\}$ is called a *Covering System* if every integer $n \in \mathbb{Z}$ satisfies at least one of the congruences.

$$\bigcup_{i=1}^{k} (a_i \pmod{m_i}) = \mathbb{Z} \tag{1}$$

The most famous example involves moduli $\{2, 3, 4, 6, 12\}$.

2.2 The Dynamic Modulus Map

We define a cryptographic state transition function $T : \mathbb{Z} \to \mathbb{Z}$ that is driven by a Covering System $\mathcal{C}$.

Definition 1 (Covering Map)**.** *Let $\mathcal{C} = \{(a_i, m_i)\}$ be a covering system. We assign a distinct affine transformation $f_i(S) = q_i S + d_i$ to each congruence. The state evolution is defined as:*

$$S_{t+1} = f_j(S_t) \quad \textit{where } j = \min\{i \mid S_t \equiv a_i \pmod{m_i}\}$$

Because $\mathcal{C}$ covers $\mathbb{Z}$, the index j is always defined. No state is "idle."

3 Architecture: The Modulus Controller

In our hardware implementation (The "Drift" Core), a **Covering Logic Unit (CLU)** monitors the current state residue. Unlike static maps (e.g., Collatz, which always divides by 2 on evens), the CLU rotates through prime bases to maximize diffusion.

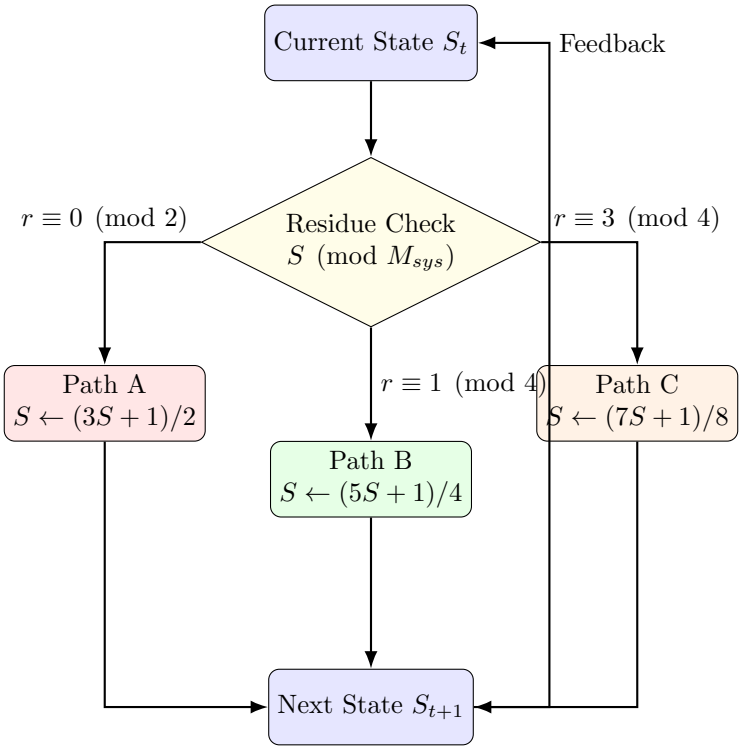

Figure 1: Logic Flow of a Dynamic Covering System. The "Residue Check" guarantees that one of the divergent paths is always selected.

4 Security Guarantees

4.1 Theorem: Absence of "Dark Corners"

Theorem 1 (Global Traversal)**.** *If the map is defined by a Covering System, there exists no integer $n \in \mathbb{Z}$ such that $T(n)$ is undefined. Furthermore, if the set of multipliers $\{q_i\}$ are distinct primes, the system minimizes the probability of invariant subspaces.*

Proof. By the definition of a covering system, $\bigcup(a_i \pmod{m_i}) = \mathbb{Z}$. Therefore, the domain of T is the entire set of integers. The system is algebraically forced to transition every state. □

4.2 Preventing Short Cycles

Standard maps allow trajectories to become trapped in "attractor basins." The Covering System mitigates this by assigning a "Kick" function (e.g., a large prime multiplier $q = 17$) to specific "trap" residues. Because the covering set is exhaustive, no state can escape this logic.

5 Conclusion

By integrating Erdős Covering Systems into the logic of Arithmetic Entropy, we create a system where ergodicity is a proven algebraic property, not a statistical assumption. This provides a formal basis for "Backdoor-Free" cryptography.